ISSN: 2454-9940

# INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 3, 2025

# Elliptic Curve Cryptography: A Safe Method for Encrypting Data in the Cloud

[1] Pattela Hemalatha, 2 Dondeti Rammohanreddy

[1] PG Scholar, Dept of CSE, NEWTONS INSTITUTE OF ENGINEERING COLLAGE, MACHERLA.

[2] Assocate Professor Dept of CSE, NEWTONS INSTITUTE OF ENGINEERING COLLAGE, MACHERLA.

## Abstract—

***It is commonly believed that cloud computing, which is constantly evolving, will be the computer architecture of the future. With the use of cloud computing, users are able to save their files and programs on a distant server network. Amazon Web Services, Rackspace, VMware, iCloud, Dropbox, Google Apps, and Microsoft Azure are just a few of the cloud service providers that let their clients build and launch their own apps on the cloud. Another perk of these service providers is that they let consumers access and utilize their apps from anywhere in the globe. Concerning modern times, the issue of security presents considerable obstacles. Building trust between cloud service providers and data owners inside the cloud is the main goal of cloud security. Protecting the authenticity and integrity of user data is the responsibility of the cloud service provider. Cloud security may therefore be adequately guaranteed by using a number of encryption methods. When it comes to protecting sensitive information, data encryption is a standard practice. With an emphasis on its use in digital signature and encryption procedures, this research examines the Elliptic Curve Cryptography technique. Improving the safety of cloud applications is the goal. Key sizes, CPU time requirements, and memory utilisation are all lowered using elliptic curve cryptography, making it an extremely effective and resilient encryption solution.***

***Keywords— Cloud computing; data security; encryption; cryptography; ECC***

## INTRODUCTION

Networks, servers, storage, applications, and services are all part of a common pool of programmable computing resources that may be easily accessed via cloud computing, according to NIST [1]. There is little to no effort or dependency on service providers for the quick provisioning and release of these resources. This innovation makes it easier to store user information and applications on remote servers, which opens up availability of these resources from any place over the internet [2]. Users are able to access their data remotely from any machine with an internet connection and use their applications without installing anything [3]. By pooling resources like memory, storage, processors, and bandwidth, this technology makes computing more efficient. Numerous service models are available with cloud computing. These include software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Many important traits are present in cloud computing. One of them is on-demand self-service, which lets customers control their own computer resources whenever they need them [4]. In addition, it provides extensive network connectivity, so customers may access the cloud services from a variety of devices and platforms. Another essential feature is resource pooling, which enables several users to dynamically share and distribute resources [5]. Additionally, Cloud Computing provides rapid elasticity, which allows for the efficient and rapid scaling of resources according to demand. Finally, it offers metered service, which lets you keep tabs on your resources and adjust them as needed for more precise pricing and allocation. Public, private, hybrid, and community clouds are some of the deployment options that make up the cloud computing environment, which provides access to computer resources [6]. Search Terms—ECC, cloud computing, data security, encryption I. Greetings Networks, servers, storage, applications, and services are all part of a common pool of programmable computing resources that may be easily accessed via cloud computing, according to NIST [1]. There is little to no effort or dependency on service providers for the quick provisioning and release of these resources. Trusted computing methods and cryptographic algorithms are therefore essential for cloud computing security. Data encryption and decryption are processes that cryptography is in charge of carrying out. Factors like as data protection, governance, incident response, compliance, and availability are all part of cloud data security [7].

## DATA SECURITY MODEL

Issues with data access, confidentiality, location, and integrity arise when dealing with delivery and deployment strategies. Three fundamental security objectives—confidentiality, integrity, and availability—make up the CIA triad, a well-known security architecture [8]. Data and information security, together with the security of computer services, are the focus of these goals. Implementing effective identity management practices, bolstering network security to prevent unauthorized access or malicious activities, and highlighting the adoption of multi-factor authentication for enhanced security are

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 3, 2025

additional security goals commonly observed in various systems that deal with system failures or data loss [9].

## Data Confidentiality and Privacy

Users may choose to store various kinds of information, such data and videos, with either one or many cloud providers, and their data is stored on several remote servers [10]. Protecting user information while it is stored on a remote server is of the utmost importance. The term "data" is used to describe a set of numerical or descriptive information. Private information is shielded from unauthorized individuals, techniques, and devices by the concept of confidentiality. Confidentiality is essential for the protection and integrity of information. Service providers have a responsibility to safeguard users' personal information by enforcing strict controls on the dissemination of personally identifiable information and other sensitive data[11].

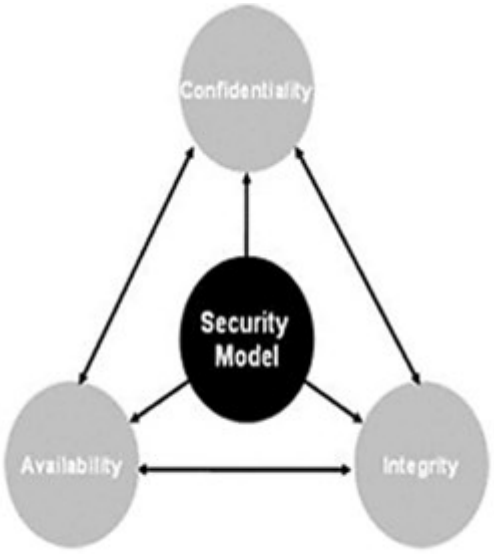


Fig. 1. Data security model

## Data Integrity

Data integrity is a must for cloud service providers looking to earn their customers' trust. Making sure the system is functioning correctly and that user data is not misused is part of it [12]. The cloud provider also has an obligation to meticulously document the whereabouts, storage capacity, and virtual machines of all cloud data [13]. Accountability and openness strengthen confidence between providers and consumers. Reliable and secure cloud services, as well as the privacy of user data, rely on a solid data integrity architecture [14].

## Data Availability

The availability of data depends on its partitioning and distribution over several servers to provide recovery in the event of a site failure or natural catastrophe [15]. Making sure that only approved users or organizations have access to sensitive information is a key component of data availability in the cloud. incorporate strong authentication and authorization procedures, encrypt data to protect sensitive information, take appropriate measures to ensure data integrity, and make data recovery easier in the case of a computer security breach. The degree of security is impacted by whether the data centers are internal or third-party. Access to data is assured at all times. Numerous elements guarantee data availability. Included in this category are things like access, file systems, recovery roles, processing overhead, and service level agreements (SLAs). Availability ensures that authorized users may access services and that the system runs efficiently. Backup, recovery, and data storage are the three pillars upon which data availability rests. Providers of services should at least provide storage options based on RAID.

## Data location and relocation

Because it is frequently moved to other virtual machines, the data stored in cloud computing systems is very mobile. The cloud service provider is responsible for providing an adequate level of security to suit the needs of their different clientele. Some people may not be aware of where their data is stored if they lack expertise or experience. Nonetheless, large businesses may pick and choose which regions to store their data in. via such cases, enterprises must ensure that the cloud service provider and themselves are legally bound to one another via a legally binding agreement.

## SECURITY ISSUES IN CLOUD

Unauthorized access to sensitive data, insufficient data segregation, a lack of accountability, software vulnerability exploitation, data recovery challenges, hostile insiders, and other similar issues are some of the many areas that cloud computing security concerns fall into. Regulatory compliance is a common area of worry when it comes to cloud computing security. Despite requests for security certifications and checks, some service providers may fight back. Another big problem is privilege user access, which lets authorized users see sensitive data that is controlled by someone else. This method is not without its risks. Clients could be unaware of the

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 3, 2025

physical location of their data servers. Client data is kept apart from data belonging to other customers using cloud data segregation. Agreements between service providers are vital for disaster recovery. When investigating possible malfeasance, cloud computing may impede investigative assistance. As a client, you should think about how your data will hold up after an incident. Take care of the following security concerns to keep data secure, intact, and accessible in the cloud: 1. Key management: the process of safely creating, distributing, storing, and revoking cryptographic keys that are used for cloud-based data encryption and decryption. 2. Controlling who has access to what in the cloud is what access control is all about. Thirdly, searchable encryption techniques are cryptographic approaches that keep the entire dataset secret while allowing users to search and retrieve particular information from encrypted data stored in the cloud. Without physically accessing the system or data, remote integrity tests may confirm its integrity. A few examples of verification techniques include cryptographic hashes, digital signatures, and checksums. Nonetheless, evidence of ownership certifies that a person has the right to own or control an item.

## PROPOSED WORK

In order to encrypt data, Victor Miller and Neil Koblitz created ECC. ECC uses elliptic curve theory–based cryptographic keys to implement public-key cryptography quickly and effectively. In order to encrypt data, Elliptic Curve Cryptography (ECC) makes use of mathematical group equations and elliptic curves. This collection of values may be used to construct a third value; it consists of the points where a line intersects the axes. When compared to other encryption technologies, Elliptic Curve Cryptography (ECC) offers superior security and makes attacks more difficult. Elliptic Curve Cryptography (ECC) is useful for smart cards, pagers, and mobile phones as it offers the same level of security while using less power, battery life, and memory. ECC is more suitable for usage on mobile devices because to its speed. When it comes to cryptographic characteristics, elliptic curves are superior.

## Choice of Field

An elliptic curve is a smooth cubic curve with two variables represented as f(x,y) = 0, and it is defined over a field K. A rational point, which may stand for infinity, is included in this curve. K is a field that contains many different kinds of mathematical objects, such as real numbers, complex numbers, rational numbers, extensions of rationals, p-adic numbers, and finite fields. The study of elliptic curve groups with respect to cryptography applications is on studying these groups over the basic fields of Fp. Here is an equation that shows how an elliptic curve is represented:

$$y^2 = x^3 + ax + b \quad (1)$$

Where, x, y is the co-ordinates and a, b are constant values.

Consider the elliptic curve

$$E: Y^2 = X^3 - X + 1 \quad (2)$$

The points P1 and P2 is added on E, by

$$P3 = P1 + P2 \quad (3)$$

Where E is the elliptic curve and P is the point on the curve

As shown in picture. Let P1=(x1, y1), P2=(x2, y2), P3=(x3, y3) and P1 not equals P2

$$m = \frac{y_2 - y_1}{x_2 - x_1};$$

To find the intersection with E. we get

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

$$or, 0 = x^3 - m^2x^2 + \ldots$$

$$So, x_3 = m^2 - x_1 - x_2$$

$$\Rightarrow y_3 = m(x_1 - x_2) - y_1$$

Multiplication is defined by the following curve, i.e 3P=P+P+P

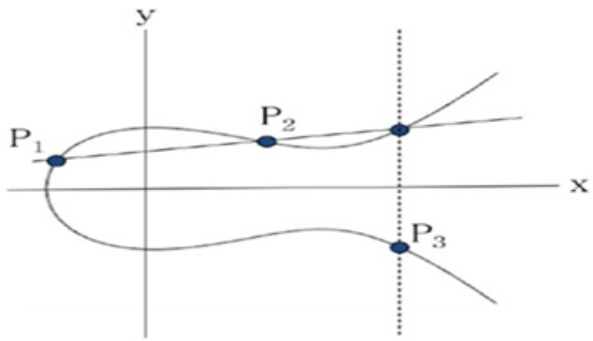


Fig. 2. Elliptic Curve

## Method

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 3, 2025

Every step of elliptic curve cryptography—key generation, encryption, decryption, and proof—is important. The first step is to create cryptographic keys. The generation of cryptographic keys is crucial. Public and private keys need to be generated via algorithms. With the recipient's public key, the sender can encrypt the communication, and with the private key, the receiver can decode it. Assuming that 'd' is an integer between 1 and n-1, 'P' is a curve point, 'Q' is the public key, and 'd' is the private key, the equation Q = d * P is used to generate the public key 'Q'. The set of numbers from 0 to n is used as a random variable.

Q = d * P

The random number d may be anything from one to n-1. On a curve, P is the point. Q denotes the public key, whereas d denotes the private key.

## Encryption

Encrypt using ECC using the public key of the receiver. Ciphertexts (C1, C2) and a random integer (k) are necessary for ECC encryption.

## Decryption

To recover the original message, the recipient needs the private key (d) to decipher the ciphertexts.

## Proof

With the recipient's private key, they may decipher the ciphertexts and recover the original message (d).

# PERFORMANCE ANALYSIS

In this part, we compare our system to the RSA scheme in terms of block size, key size, and other attributes. In order to assess two cryptographic methods, this comparison uses the same set of security parameters.

## Block Size

We anticipate the following RSA block sizes in practice. In terms of key size, the block sizes used by ECC and RSA are identical. A block size of ((ks/8) - 11) is used during encryption, whereas a block size of (ks/8) is used during decryption.

## Key Size

The key sizes and security levels of the Elliptic Curve Cryptography (ECC) and Rivest-Shamir Adleman (RSA) algorithms were tested in accordance with the standards set by NIST. Key sizes and degrees of security for ECC and RSA are compared in the table below.

TABLE 1. KEY SIZES WITH EQUIVALENT SECURITY LEVELS

| ECC (bits) | RSA (bits) | Key size ratio |
|---|---|---|
| 128 | 512 | 1:8 |
| 164 | 1024 | 1:12 |
| 232 | 2048 | 1:20 |
| 356 | 3062 | 1:24 |
| 512 | 6048 | 1:30 |

## Parameters

Time needed for key generation, encryption, and decryption are crucial considerations in cryptographic systems; they are the characteristics used to assess the features of both the RSA and ECC algorithms. The evaluation and performance of these systems are greatly impacted by these three-time measures. It is possible to run the tests again, recording times, while keeping an eye on all three of these elements separately. This leads to the examination of average duration.

# METHODOLOGY

The following steps outline how to use the Elliptic Curve Cryptography method in a cloud setting. Producing an app for Google Play is the starting point. You need to visit http://accounts.google.com/ in order to begin the process of making an account. The user must provide their username and password in order to access the website. The next step is for the user to choose their own program, which is Step 2. To see the applications I have submitted, please click on the provided link. Finally, in Step 3, choose "Create Application." Before they can click the "Create Application" button, they need to provide the application identification and title. The application process has begun. Step four involves creating a database using Google Cloud SQL or any suitable solution. Step five requires the user to choose "New instance" and then provide the name of the instance along with an application that has already been created. After that, find the "Create Instance" option and press the button. Next, choose the instance name to see its associated attributes. To have all databases load automatically, go to the "SQL Prompt" tab. Step eight involves creating the database and tables using SQL queries, and then inserting records. Building the program's user interface is the next stage. As part of the eleventh stage, you'll need to write some Java

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 3, 2025

code that makes good use of the ECC method. In addition, the program's debugging procedure must be carried out inside the Google Cloud environment. The next step is to encrypt the data before storing it safely. If the data is accessible, it has to be shown after decryption.

## Execution Flow

In a cloud environment, the user's sensitive data is safely stored by the service provider. The technology creates a public and private key pair once data is stored in the cloud. Following this, the method is encrypted using the ECC procedure. It produces ciphertext as a result. The recipient's job is to decrypt the encrypted message. Initial contact will be established.

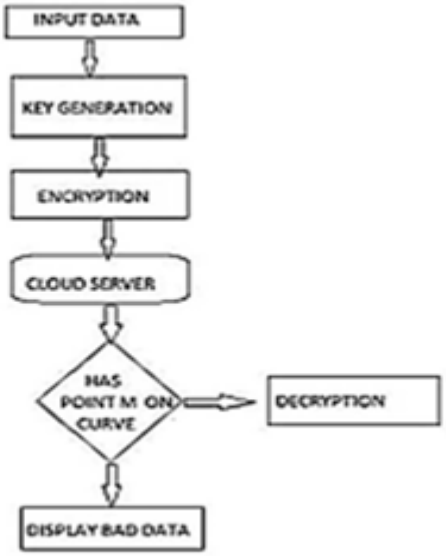


Fig.3. Execution Flow

## CONCLUSION

This study delves into the security issues related to user data in the cloud and emphasizes the need of finding a solution. Elliptic Curve Cryptography (ECC) is a reliable and secure architecture that may be used to build and deploy applications in the cloud. When compared to linear methods, the ECC algorithm improves security since it offers faster processing at lower computational cost. Because it can provide the same degree of security with lower key lengths, Elliptic Curve Cryptography (ECC) has significant benefits over RSA. Many communication applications employ Elliptic Curve Cryptography (ECC), including picture encryption, server-based encryption, wireless sensor networks, and mobile computing.

*REFERENCES*

*[1] Y. Chen, Y. Lin, Y. Hu, S. Member, and C. Hsia, "Distributed Real-Time Object Detection Based on Edge-Cloud Collaboration for Smart Video Surveillance Applications," IEEE Access, vol. 10, no. September, pp. 93745–93759, 10.1109/ACCESS.2022.3203053. 2022, doi:*

*[2] S. S. Ali and B. J. Choi, "State-of-the-art artificial intelligence techniques for distributed smart grids: A review," Electron., vol. 9, no. 6, pp. 1–28, 2020, doi: 10.3390/electronics9061030.*

*[3] T. J. Nandhini and K. Thinakaran, "Deep Neural Network-based Crime Scene Detection with Frames," 2023 Eighth Int. Conf. Sci. Technol. Eng. Math., pp. 10.1109/ICONSTEM56934.2023.10142449.*

*[4] G. Uganya, F. D. Shadrach, I. Sudha, P. M. Krishnammal, V. Lakshmanan, and T. J. Nandhini, "Crime Scene Object Detection from Surveillance Video by using Tiny YOLO Algorithm," 2023 3rd Int. Conf. Pervasive Comput. Soc. Netw., no. October, pp. 654 659, 2023, doi: 10.1109/ICPCSN58827.2023.00114.*

*[5]N. Kaaniche and M. Laurent, "Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms," Comput. Commun., vol. 111, pp. 120–141, 2017, doi: 10.1016/j.comcom.2017.07.006.*

*[6] V. D. Ganesh and R. M. Bommi, "Materials Today : Proceedings Cutting force and surface roughness measurement in turning of Monel K 500 using GRA method," Mater. Today Proc., no. xxxx, 2023, doi: 10.1016/j.matpr.2023.05.722.*

*[7] A. Abdulridha, D. Salama, and K. M, "NHCA: Developing New Hybrid Cryptography Algorithm for Cloud Computing Environment," Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 11, pp. 479–486, 2017, doi: 10.14569/ijacsa.2017.081158.*

*[8] S. Berlato, R. Carbone, A. J. Lee, and S. Ranise, "Exploring Architectures for Cryptographic Access Control Enforcement in the Cloud for Fun and Optimization," Proc. 15th ACM Asia Conf. Comput. Commun. Secur. ASIA CCS 2020, pp. 208–221, 2020, doi: 10.1145/3320269.3384767.*

*[9]A. N. Jaber and M. F. Bin Zolkipli, "Use of cryptography in cloud computing," Proc. - 2013 IEEE Int. Conf. Control Syst. Comput. Eng. ICCSCE 2013, no. May 2016, pp. 179–184, 2013, doi: 10.1109/ICCSCE.2013.6719955.*

*[10]N. E. El-Attar, D. S. El-Morshedy, and W. A. Awad, "A New Hybrid Automated Security Framework to Cloud Storage System," Cryptography, vol. 5, no. 4, p. 37, 2021, doi: 10.3390/cryptography5040037.*

*[11] S. Caleb and S. J. J. Thangaraj, "Data-driven ML Approaches for the concept of Self-healing in CWN , Including its Challenges and Possible Solutions," 2023 Eighth Int. Conf. Sci. Technol. Eng. Math., pp. 1–7, doi: 10.1109/ICONSTEM56934.2023.10142451.*

*[12] R. Latha, "Deauthentication Attack Detection in the Wi-Fi network by Using ML Techniques," 2022.*

*[13] H. Du, J. Chen, M. Chen, C. Peng, and D. He, "A Lightweight Authenticated Searchable Encryption without Bilinear Pairing for Cloud Computing," Wirel. Commun. Mob. Comput., vol. 2022, 2022, doi: 10.1155/2022/2336685.*

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 3, 2025

*[14] R. Rastogi and M. S. Sheela, "Enhancement of Channel Capacity in 5G Ultra Dense Network-UDN," 2023 2nd Int. Conf. Edge Comput. Appl., no. Icecaa, pp. 303–307, 2023, doi: 10.1109/ICECAA58104.2023.10212363.*

*[15]N. Nalini and I. Ahmed, "Network Intrusion Detection System for Feature Extraction based on Machine Learning Techniques," 2023 5th Int. Conf. Inven. Res. Comput. Appl., no. Icirca, pp. 440–445, 2023, doi: 10.1109/ICIRCA57980.2023.10220789.*